Data Protection Policy

January 2024
Review January 2025

Contents:

Statement of intent

Westhoughton High School is required to keep and process certain information about its staff members, students, parents, governors, visitors and other individuals in accordance with its legal obligations.

The school may, from time to time, be required to share personal information about its staff or students with other organisations, mainly the LA, DfE, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and Westhoughton High School believes that it is good practice to keep clear practical policies, backed up by written procedures.

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

1 Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA)
- The Freedom of Information Act 2000
- The Education (Student Information) (England) Regulations 2005 (as amended in 2018)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Protection of Freedoms Act 2012
- DfE (2023) 'Keeping Children Safe in Education 2023'

This policy will also have regard to the following guidance:

- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2023) 'Data protection in schools'

This policy will be implemented in conjunction with the following other school policies:

- Privacy notices (staff & students)
- E-safety Policy
- Acceptable Usage
- Freedom of Information Policy
- Surveillance and CCTV Policy
- Child Protection and Safeguarding Policy

2 Applicable data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. names (including initials), identification numbers, a username, an IP address or a job description. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

'Sensitive personal data' is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
    - Racial or ethnic origin.
    - Political opinions.
    - Religious or philosophical beliefs.
    - Trade union membership.
    - Principles.

'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law.

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles.

3. Accountability

Westhoughton High School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

The school will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data
- Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures in place to protect the personal data
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The school will also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches

The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.
- Regularly training employees on data protection law, this policy, any related policies and any other data protection matters. The school will maintain a record of training attendance by employees.

Data protection impact assessments (DPIAs) will be used to identify and reduce data protection risks, where appropriate.

4. Data Protection Officer (DPO)

Schools are required to appoint a DPO who will be the central point of contact for all data subjects and others in relation to matters of data protection.

A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the school's compliance with the UK GDPR, the DPA and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.

The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the school's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.

- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the school community.
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.

An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

The DPO will report to the highest level of management at the school, which is the Headteacher.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their UK GDPR obligations.

The DPO will report to the highest level of management at the school, which is the governing board.

Staff will ensure that they involve the DPO in all data protection matters closely and in a timely manner.

5. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, personal data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the school in the performance of its tasks

The school will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
    - Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law
- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared, and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right of the data subject to raise a complaint with the ICO in relation to any processing.

The school has privacy notices for the following groups, which outline the information above that is specific to them:

- Prospective employees
- Students and their families
- School workforce

- Third parties
- Trustees and governors
- Volunteers

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

Where the school relies on:

- 'Performance of contract' to process a child's data, the school considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- Consent to process a child's data, the school ensures that the requirements outlined in the 'Consent' section are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

6. Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The school ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained. Consent can be withdrawn by the individual at any time.

When pupils and staff join the school, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children.
In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above.

7. The right to be informed

Adults and children have the same right to be informed about how the school uses their data.

The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided. – this information will be supplied at the time the data is obtained.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

8. The right of access

Individuals, including children, have the right to obtain confirmation that their data is being processed.

Individuals, including children, have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a SAR has been made for information held about a child, the school will evaluate whether the child is capable of fully understanding their rights. If the school determines the child can understand their rights, it will respond directly to the child.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

The school will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the school will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to – the time

limit for responding to the request will be paused until clarification from the individual is received.

9. The right to rectification

Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. The school reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

The school will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. The school will restrict processing of the data in question whilst its accuracy is being verified, where possible.

Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

10. The right to erasure

Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The establishment, exercise or defence of legal claims

The school has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

Requests for erasure will be handled free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

11. The right to restrict processing

Individuals, including children, have the right to block or suppress the school's processing of personal data.

In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual

- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. The school will inform individuals when a restriction on processing has been lifted.

Where the school is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The school reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

12. The right to data portability

Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The school will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

The school will provide the information free of charge.

In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The school will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13. The right to object

The school will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Processing used for direct marketing purposes
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The school will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The school will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. The school will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

Where no action is being taken in response to an objection, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. Automated decision making and profiling

The school will only ever conduct solely automated decision making with legal or similarly significant effects is the decision is:

- Necessary for entering into or performance of a contract.
- Authorised by law.
- Based on the individual's explicit consent.

Automated decisions will not concern a child nor use special category personal data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

The school will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.

The school will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.
Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.
When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

15. Data Protection by design and default

The school will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, the school will ensure that only data that is necessary to achieve its specific purpose will be processed.

The school will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in school ICT systems.
- Implementing basic technical measures within the school network and ICT systems to ensure data is kept secure.
- Promoting the identity of the DPO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

16. Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

17. Data breaches

The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The headteacher will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Where the school faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Within a breach notification to the supervisory authority, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Where notifying an individual about a breach to their personal data, the school will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

The school will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

The school will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

18. Data security

The school will keep personal data secure by taking appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage. In particular:

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Westhoughton High School takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The DPO is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Employees must follow all procedures and technologies the school puts in place to maintain the security of all personal data from the point it is collected to the point it is destroyed.

Employees must also comply with all applicable aspects of the school's [Acceptable Usage Policy] and not attempt to circumvent the administrative, physical and technical safeguards the school implements and maintains in accordance with the UK GDPR and the DPA.

The school will introduce a protective marking scheme to ensure that all data – electronic or on paper – is labelled according to the protection it requires based on Impact Levels:

Impact level	**Impact**	**Colour Code**	**Memory stick?**	**Example**
IL0–Not Protectively Marked	No harm or embarrassment will occur if items become public knowledge		Yes	Newsletters, public information
IL1- Unclassified			Yes	Generic letters to parents containing no personal data
IL2–PROTECT	Some harm or embarrassment will occur if items become public knowledge		No	Basic student information such as name and address
IL3–Restricted	Harm or embarrassment will occur if items become public knowledge		No	Sensitive Student information such as ethnicity or FSM status
IL4-Confidential	Serious harm or embarrassment will occur if items become public knowledge		No	Highly sensitive student data relating to child protection

An Information Risk Register will be created and maintained by the school which summarises each information asset the school maintains. Appropriate measures will be taken to mitigate the risk of disclosure of each information asset based on the impact level assigned. The information risk register can be found in **Appendix 1.**

19. Safeguarding

Westhoughton high School understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

The school will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils. The governing board will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.

- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.

The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

The school will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

Students' personal data will not be provided where the serious harm test is met. Where there is doubt, the school will seek independent legal advice.

20. Publication of information

Westhoughton High School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

Westhoughton High School will not publish any personal information, including photos, on its website without the permission of the affected individual.
When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. CCTV and photography

The Surveillance & CCTV Policy explains the rationale fully for use of CCTV on the school site.

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The school notifies all students, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for six months for security purposes; the DPO is responsible for keeping the records secure and allowing access.

The school will always indicate its intentions for taking photographs of students and will retrieve permission before publishing them.

If the school wishes to use images/video footage of students in a publication, such as the school website, prospectus, or recordings of school plays, Consent records will be checked.

Precautions are taken when publishing photographs of students, in print, video or on the school website.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

22. Cloud computing

For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the school's policies for the use of cloud computing.

The school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which

the service provider may access the personal data it processes, such as the provision of support services.

The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the school's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.

- Monitor the use of the school's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher

23. Data retention

Data will not be kept for longer than is necessary and in accordance with the school's retention schedule (see Appendix 1).

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former students or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained in accordance with the school's retention schedule (see Appendix 1).

24. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

25. Monitoring and review

This policy is reviewed every two years by the DPO and the Headteacher, and ratified by the Governing Body.

Appendix 1
Information Risk Register
NOTE TO SCHOOLS:
This retention schedule is based on guidance from the records management society:
http://www.irms.org.uk/images/resources/infoguides/records_management_toolkit_for_schools_version_4_may_2012.pdf

The Data Protection Officer is Mrs Gillian Bailey. S/he is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements. This includes:

1 Owning and updating this policy
2 Owning the information risk register
3 Appointing Information Asset Owners (IAOs) for each Information Asset
4 Advocating information risk management and raising awareness of information security issues
5 After liaising with the Local Authority decide if a security incident is of sufficient severity to report to the information Commissioners Office.

Information Asset Owners are responsible for:
6 Ensuring the information is used for the purpose it was collected
7 How information has been amended or added to over time
8 Who has access to protected data and why

Named Information Asset Owners are:

HT	Head Teacher
DH (P)	Deputy Head Pastoral
DH (C)	Deputy Head Curriculum
CtG	Clerk to Governors
SBM	School Business Manager
IND	Individual staff
AS	Admin staff
DM	Data Manager
FM	Facilities Manager
SEN	Senco
EO	Exams Officer
EVC	Educational Visits Coordinator
BC	Bolton Council
PTA	Parent Teachers' Association

1 Child Protection

These retention periods should be used in conjunction with the document "Safeguarding Children and Safer Recruitment in Education which can be downloaded from this link:
httAS://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289214/safeguarding_children_and_safer_recruitment_in_education.pdf

IAO	Basic file description	Data Prot Issues	Statutory Provisions	Retention period [operational]	Action at the end of the administrative life of the record	Protective Marking Classification
DH(P)	Child Protection files	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	DOB + 25 years	SECURE DISPOSAL Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university for example)	**IL4-Confidential**
DH (P)	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL The following is an extract from "Safeguarding Children and Safer Recruitment in Education" p60 "Record Keeping 5.10 It is important that a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on a person's confidential personnel file, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference if the person has moved on. It will provide clarification in cases where a future CRB Disclosure reveals information from the police about an allegation that did not result in a criminal conviction. And it will help to prevent unnecessary reinvestigation if, as sometimes happens, an allegation re-surfaces after a period of time. The record should be retained at least until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer."	**IL4-Confidential**

2 Governors						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
	Minutes					
CtG	*Principal set (signed)*	No		Permanent	Retain in school whilst school is open then transfer to Archives.	**IL3 - RESTRICTED**
CtG	*Inspection copies*	No		Date of meeting + 3 years	If these minutes contain any sensitive persona information they should be SECURELY DISPOSED	**IL3 - RESTRICTED**
CtG	Agendas	No		Date of meeting	SECURE DISPOSAL	**IL1–Unclassified**
CtG	Reports	No		Date of report + 6 years	SECURE DISPOSAL	**IL1–Unclassified**
CtG	Annual Parents' meeting papers	No		Date of meeting + 6 years	SECURE DISPOSAL	**IL1–Unclassified**
CtG	Instruments of Government	No		Permanent	Retain in school whilst school is open then transfer to Archives.	**IL1–Unclassified**
SBM	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required then transfer to Archives.	**IL1–Unclassified**
HT	Action Plans	No		Date of action plan + 3 years	SECURE DISPOSAL	**IL1–Unclassified**

CtG	Statutory Policy documents (does not include school specific policies such as writing policies etc.)	No		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process) SECURE DISPOSAL	**IL1–Unclassified**
HT	Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years. Review for further retention in the case of contentious disputes. SECURE DISPOSAL	**IL3 - RESTRICTED**

3 Management						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
CtG	Minutes of the Senior Management Team and other internal administrative bodies	Yes[1]		Date of meeting + 5 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
CtG	Reports made by the head teacher or the management team	Yes[1]		Date of report + 3 years	SECURE DISPOSAL	**IL3 - RESTRICTED**

IND	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes[1]		Closure of file + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
IND	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	No		Date of correspondence + 3 years	SECURE DISPOSAL	**IL2–PROTECT**
CtG	Professional development plans (Management plans for professional development plans of staff)	Yes		Closure + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
CtG	School development plans	No		Closure + 6 years	Review Offer to the Archives	**IL2–PROTECT**

AS	Admissions – if the admission is successful	Yes		Admission + 1 year	SECURE DISPOSAL	**IL3 - RESTRICTED**
AS	Admissions – if the appeal is unsuccessful	Yes		Resolution of case + 1 year	SECURE DISPOSAL	**IL3 - RESTRICTED**
AS	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL	**IL3 - RESTRICTED**
AS	Proofs of address supplied by parents as part of the admissions process	Yes		Current year + 1 year	SECURE DISPOSAL	**IL3 - RESTRICTED**
[1] From January 1st 2005 subject access is permitted into unstructured filing systems and log books and other records created within the school containing details about the activities of individual students and members of staff will become subject to the GDPR and the Data Protection Act 2018.						
AS	Admission Registers	Yes		Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry. Offer to the Archives	**IL3 - RESTRICTED**
DM	Attendance registers	Yes	The Education (Student Registration) (England) Regulations 2006 (No. 1751)	Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any backup copies should be destroyed at the same time]	**IL3 - RESTRICTED**

DM	Student record cards	Yes	Limitation Act 1980	DOB of the student + 25 years[1]	SECURE DISPOSAL	**IL3 - RESTRICTED**
DM	Student files	Yes	Limitation Act 1980	DOB of the student + 25 years[2]	SECURE DISPOSAL	**IL3 - RESTRICTED**
SEN	Special Educational Needs files, reviews and Individual Education Plans	Yes		DOB of the student + 25 years	SECURE DISPOSAL NOTE: This retention period is the minimum period that any student file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.	**IL4-Confidential**
AS	Correspondence Relating to Authorised Absence and Issues	No		Date of absence + 2 years	SECURE DISPOSAL	**IL2–PROTECT**
EO	Examination results - Public	No		Year of exams + 6 years	SECURE DISPOSAL Any certificates left unclaimed should be returned to the appropriate Examination Board	**IL2–PROTECT**
DH (C)	Internal examination results	Yes		Current year + 5 years[3]	SECURE DISPOSAL	**IL2–PROTECT**

HT	Any other records created in the course of contact with students	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL	**IL3 - RESTRICTED**
SEN	EHCP maintained under The Education Act 1996 - Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 31 years	SECURE DISPOSAL unless legal action is pending	**IL4-Confidential**
SEN	Proposed EHCP or amended EHCP	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 31 years	SECURE DISPOSAL unless legal action is pending	**IL4-Confidential**
SEN	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	6 months paper copy Closure + 12 years	SECURE DISPOSAL unless legal action is pending	**IL4-Confidential**
SEN	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	6 months paper copy Closure + 12 years	SECURE DISPOSAL unless legal action is pending	**IL3 - RESTRICTED**

SEN	Children's SEN Files	Yes		6 months paper copy DOB of student + 25 years then review – it may be appropriate to add an additional retention period in certain cases	SECURE DISPOSAL unless legal action is pending	**IL4-Confidential**
EVC	Parental permission slips for school trips – where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL	**IL3 - RESTRICTED**
EVC	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980	DOB of the student involved in the incident + 25 years The permission slips for all students on the trip need to be retained to show that the rules had been followed for all students	SECURE DISPOSAL	**IL3 - RESTRICTED**

EVC	Records created by schools to obtain approval to run an Educational Visit outside the Classroom	N	3 part supplement to the Health & Safety of Students on Educational Visits (HASPEV) (1998).	Date of visit + 10 years[7]	SECURE DISPOSAL or delete securely	**IL2–PROTECT**

[1] In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service

[2] As above

[3] If these records are retained on the student file or in their National Record of Achievement they need only be kept for as long as operationally necessary.

[4] This retention period has been set in agreement with the Safeguarding Children's Officer

4 Curriculum						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
DH (C)	Curriculum development	No		Current year + 6 years	SECURE DISPOSAL	**IL1–Unclassified**
DH (C)	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL	**IL1–Unclassified**
DH (C)	School syllabus	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL1–Unclassified**

DH (C)	Schemes of work	No		Current year + 1 year This retention period starts once the document has been superseded	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL1–Unclassified**
DH (C)	Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL1–Unclassified**
IND	Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL2–PROTECT**
IND	Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL2–PROTECT**
IND	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL2–PROTECT**
IND	Students' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL2–PROTECT**

DH (C)	Examination results	Yes		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
DH (C)	SATS records	Yes		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
DH (C)	PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
DH (C)	Value added records	Yes		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
HT	Self-Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**

5 Personnel Records held in Schools						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
SBM	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Staff Personal files	Yes		Termination + 7 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Interview notes and recruitment records	Yes		Date of interview + 6 months	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Pre-employment vetting information (including DSB Checks)	No	DBS Guidelines	Date of check + 6 months	SECURE DISPOSAL [by the designated member of staff]	**IL2–PROTECT**

SBM	Single Central Record	Yes	ISA guidelines	Keep until school closure	Offer to local authority designated officer	**IL2–PROTECT**
SBM	Disciplinary proceedings:		**Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.**			
SBM	*oral warning*	Yes		Date of warning + 6 months	SECURE DISPOSAL	**IL2–PROTECT**
SBM	*written warning – level one*	Yes		Date of warning + 6 months	SECURE DISPOSAL	**IL2–PROTECT**
SBM	*written warning – level two*	Yes		Date of warning + 12 months	SECURE DISPOSAL	**IL2–PROTECT**
SBM	*final warning*	Yes		Date of warning + 18 months	SECURE DISPOSAL	**IL2–PROTECT**
SBM	*case not found*	Yes		If child protection related please see 1.2 otherwise SECURE DISPOSAL immediately at the conclusion of the case		**IL2–PROTECT**
SBM	Records relating to accident/injury at work	Yes		Date of incident + 12 years	In the case of serious accidents a further retention period will need to be applied. SECURE DISPOSAL	**IL2–PROTECT**
CtG	Annual appraisal/assessment records	No		Current year + 5 years	SECURE DISPOSAL	**IL2–PROTECT**
BC	Salary cards	Yes		Last date of employment + 85 years	SECURE DISPOSAL	**IL2–PROTECT**

BC	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year, +3yrs	SECURE DISPOSAL	**IL2–PROTECT**
BC	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Proof of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes			Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file.	**IL2–PROTECT**

[1] If this is placed on a personal file it must be weeded from the file.

6 Health and Safety						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**

SBM	Accessibility Plans	No	Equality Act	Current year + 6 years	SECURE DISPOSAL	**IL1–Unclassified**
SBM	*Adults (All Accidents)*	Yes		Date of incident + 7 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
SBM	*Children (All Accidents)*	Yes		DOB of child + 25 years[1]	SECURE DISPOSAL	**IL3 - RESTRICTED**
FM	COSHH	No		Current year + 10 years [where appropriate an additional retention period may be allocated]	SECURE DISPOSAL	**IL1–Unclassified**
FM	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
FM	Policy Statements	No		Date of expiry + 1 year	SECURE DISPOSAL	**IL1–Unclassified**
FM	Risk Assessments	No		Current year + 3 years	SECURE DISPOSAL	**IL1–Unclassified**
FM	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No		Last action + 40 years	SECURE DISPOSAL	**IL1–Unclassified**

FM	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation	No		Last action + 40 years	SECURE DISPOSAL	**IL1–Unclassified**
FM	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL	**IL1–Unclassified**

[1] A child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the student reaches the age of 25 this retention period has been applied.

7 Administrative						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
SBM	Employer's Liability certificate	No		Closure of the school + 40 years	SECURE DISPOSAL	**IL1–Unclassified**
FM	Inventories of equipment and furniture	No		Current year + 6 years	SECURE DISPOSAL	**IL1–Unclassified**

SBM	General administrative records (records not specifically listed elsewhere)	No		Current year + 5 years	Review to see whether a further retention period is required	**IL1–Unclassified**
CtG	School brochure or prospectus	No		Current year + 3 years		**IL1–Unclassified**
SBM	Circulars (staff/parents/ students)	No		Current year + 1 year	SECURE DISPOSAL	**IL1–Unclassified**
SBM	Newsletters, ephemera	No		Current year + 1 year	Review to see whether a further retention period is required	**IL1–Unclassified**
SBM	Visitors book	No		Current year + 2 years	Review to see whether a further retention period is required	**IL1–Unclassified**

8 Finance						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
SBM	Annual Accounts	No	Financial Regulations	Current year + 6 years	Offer to the Archives	**IL2–PROTECT**

SBM	Loans and grants	No	Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required	**IL2–PROTECT**
	Contracts					
SBM	under seal	No		Contract completion date + 12 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	under signature	No		Contract completion date + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	monitoring records (Bolton Council Corporate Property Unit may hold these records on the schools behalf)	No		Current year + 2 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Copy orders	No		Current year + 2 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Budget reports, budget monitoring etc	No		Current year + 3 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Invoice, receipts and other records covered by the Financial Regulations	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**

SBM	Annual Budget and background papers	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Order books and requisitions	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Delivery Documentation	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Debtors' Records	No	Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	School Fund – Cheque books	No		Current year + 3 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	School Fund – Paying in books	No		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**
SBM	School Fund – Ledger	No		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**
SBM	School Fund – Invoices	No		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**
SBM	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	School Fund – Bank statements	No		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**
SBM	School Fund – School Journey books	No		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**

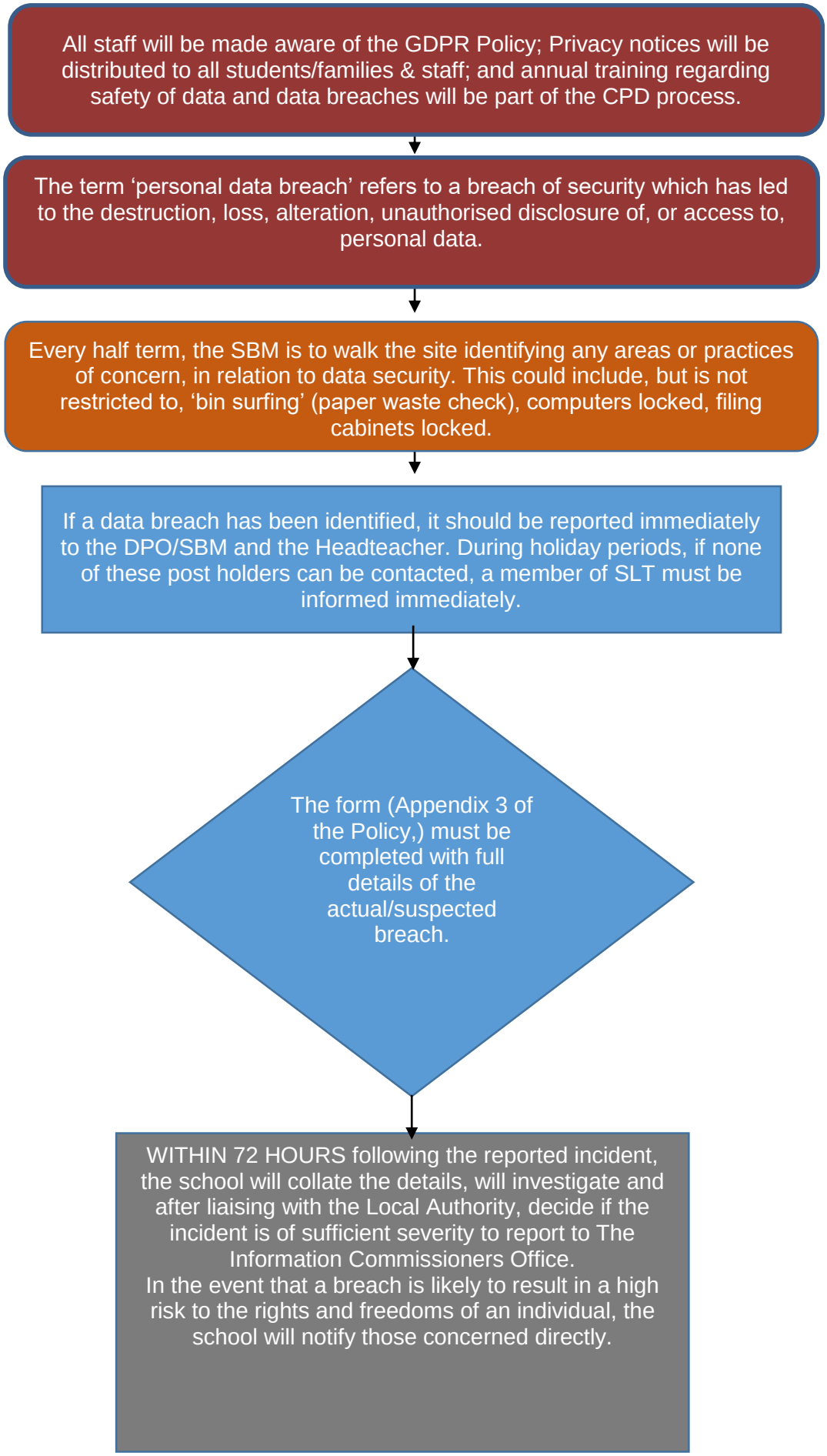
SBM	Student Grant Applications	Yes		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Free school meals registers	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
SBM	Petty cash books	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**

9 Property						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
SBM	Title Deeds	No		Permanent	Permanent -these should follow the property unless the property has been registered at the Land Registry	**IL2–PROTECT**
SBM	Plans	No		Permanent	Retain in school whilst operational	**IL3 - RESTRICTED**
SBM	Maintenance and contractors	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Leases	No		Expiry of lease + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Lettings	No		Current year + 3 years	SECURE DISPOSAL	**IL2–PROTECT**
SBM	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**

SBM	Maintenance log books	No		Last entry + 10 years	SECURE DISPOSAL	**IL1–Unclassified**
SBM	Contractors' Reports	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**

10 Department for Children, Schools and Families						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
CtG	OFSTED reports and papers	No		Replace former report with any new inspection report	Schools may wish to retain copies of former reports for longer	**IL2–PROTECT**
SBM	Returns	No		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
HT/ CtG	Circulars from Department for Children, Schools and Families	No		Whilst operationally required	Review to see whether a further retention period is required	**IL1–Unclassified**

Appendix 2
Procedures for identifying and reporting of data breaches



Appendix 3
Data Breach Incident Form

Part A: Breach Information

When did the breach occur (or become known)?	
Which staff member was involved in the breach?	
Who was the breach reported to?	
Date of Report:	
Time of Report:	
Description of Breach:	
Initial Containment Activity:	

Part B: Breach Risk Assessment

What type of data is involved:	Hard Copy: Yes / No Electronic Data: Yes / No
Is the data categorised as 'sensitive' within one of the following categories:	Racial or ethnic origin: Yes / No Political opinions: Yes / No Religious or philosophical beliefs: Yes / No Trade union membership: Yes / No Data concerning health or sex life and sexual orientation: Yes / No Genetic data: Yes / No Biometric data: Yes / No
Were any protective measures in place to secure the data (e.g. encryption):	Yes / No If yes, please outline:
What has happened to the data:	
What could the data tell a third party about the individual:	
Number of individuals affected by the breach:	
Whose data has been breached:	

What harm can come to those individuals:	
Are there wider consequences to consider e.g. reputational loss:	

Part C: Breach Notification

Is the breach likely to result in a risk to people's rights and freedoms?	Yes / No If Yes, then the ICO should be notified within 72 hours.
Date ICO notified:	
Time ICO notified:	
Reported by:	
Method used to notify ICO:	
Notes:	
Is the breach likely to result in a high risk to people's rights and freedoms?	Yes / No If Yes, then the individual should be notified
Date individual notified:	
Notified by:	
Notes:	

Part D: Breach Action Plan

Action to be taken to recover the data:	

Relevant governors/trustees to be notified:	Names:
	Date Notified:
Notification to any other relevant external agencies:	External agencies:
	Date Notified:
Internal procedures (e.g. disciplinary investigation) to be completed:	
Steps needed to prevent reoccurrence of breach:	

Data Breach Log

Date Reported:	Notified By:	Reported To:	Description of Breach:	Notification to ICO:	Notification to Individual(s)	Further Actions to be taken:	Reviewed by:
				Yes/No	Yes/No		
				Yes/No	Yes/No		
				Yes/No	Yes/No		

Appendix 4

Details of organisations who we share data

Details of data	Internal	External	type